사이버보안연구실

작성: 이예인

작성일자: 2024/09/11

|  |  |  |  |
| --- | --- | --- | --- |
| Security Issues of Firewall | | | |
| 저자 | Aakanksha Chopra | 저널 | JIMS |
| 리뷰 | | | |
| 요약 | * 문제인식 : 방화벽은 아래의 위협에 취약함  1. Malicious Employees (내부사용자) 2. Modem Users? 3. 개별 비밀번호 및 사용자 계정의 오용 4. 새로운 형태의 공격 5. 바이러스  * 해결방법 : 분산방화벽   + 내부 호스트마다 방화벽을 두는 방식 | | |
| 강점 | * 기존 방화벽에 대해 자세히 설명해놓음 | | |
| 약점 | * 분산방화벽이라는 해결책을 제시한 후 해결 방식에 대한 설명 부족 * 문제정의(방화벽 위협)에 대한 너무나 간략한 서술 * 방화벽 기본 개념에 방화벽 위협요소가 설명되어있다, | | |
| 해결책/아이디어 | * 분산방화벽을 통한 위협요소별 해결방안 제시 필요 | | |
| 배운점 | * 방화벽의 필터링 기준 선정방식 * 방화벽 역할: 접근제어, 로깅과 감사추적, 인증, 데이터암호화 * 바이러스를 필터링하기 위해 데이터내용까지 검사하게 되면 많은 오버헤드가 발생한다. 때문에 방화벽은 바이러스에 취약하다. * 분산 방화벽을 사용하면 각 내부 호스트가 방화벽을 가지고 있기 때문에 내부에서 어떤 호스트가 해킹당하더라도 각 호스트의 규칙에 의해 다른 호스트들은 해킹당하지 않는다. | | |
| 기타 | * 분산 방화벽 추가자료   <https://www.usenix.org/legacy/publications/login/1999-11/features/firewalls.html>   * 분산 방화벽 장점  1. 내부 사용자 방어 2. 병목현상 해결 | | |